PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-073556
(43)Date of publication of application : 12.03.2002

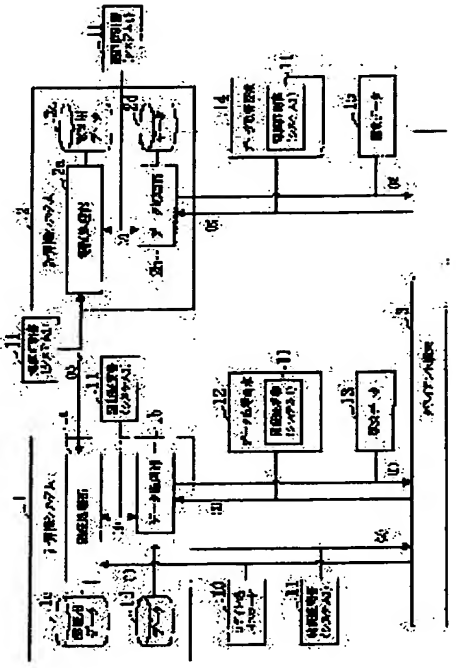
)Int.CI. G06F 15/00
G06F 15/16
G06F 15/163
G06F 15/177
G09C 1/00
H04L 9/32

)Application number : 2000-255023
)Date of filing : 25.08.2000

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : NISHIMURA TORU
HANAKI SABURO

) AUTHENTICATION SYSTEM

)Abstract:
BLEM TO BE SOLVED: To dispense with two or more times hentication works when a client terminal is to access plural puter systems and to dispense with newly installing a puter system exclusively used for authentication.
UTION: This system has a first computer system provided with irst storage device and a first authenticating processing t for performing authenticating processing and a second puter system provided with a second storage device and a ond authenticating processing part for performing henticating processing and when authenticating processing is cessful, the first and second authenticating processing parts ue a prescribed authentication certificate to a user. When user reports the authentication certificate and accesses the st or second computer system, the validity of this hentication certificate is judged by an inquiry to the puter system, which is the issuing source of this hentication certificate. When the certificate is valid, ess is permitted and when the certificate is not valid, ess is refused.



AL STATUS
te of request for examination] 13.08.2002
te of sending the examiner's decision of ection] 21.09.2004
nd of final disposal of application other n the examiner's decision of rejection or lication converted registration]

ıtė of final disposal for application]
ıtent number]
ıte of registration]
ımber of appeal against examiner's decision of
jection]
ıte of requesting appeal against examiner's
:ision of rejection]
ıte of extinction of right]

Copyright (C); 1998, 2003 Japan Patent Office

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２００２－７３５５６
（Ｐ２００２－７３５５６Ａ）
(43)公開日　平成14年3月12日(2002.3.12)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｂ	5B045
	15/16	６２０		15/16	６２０Ｂ	5B085
	15/163	６５０		15/163	６５０Ｘ	5J104
	15/177	６７０		15/177	６７０Ｃ	
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｚ	

審査請求　未請求　請求項の数２　ＯＬ　（全４頁）　最終頁に続く

(21)出願番号　特願2000-255023(P2000-255023)

(22)出願日　平成12年8月25日(2000.8.25)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号

(72)発明者　西村　徹
東京都千代田区大手町二丁目3番1号　日本電信電話株式会社内

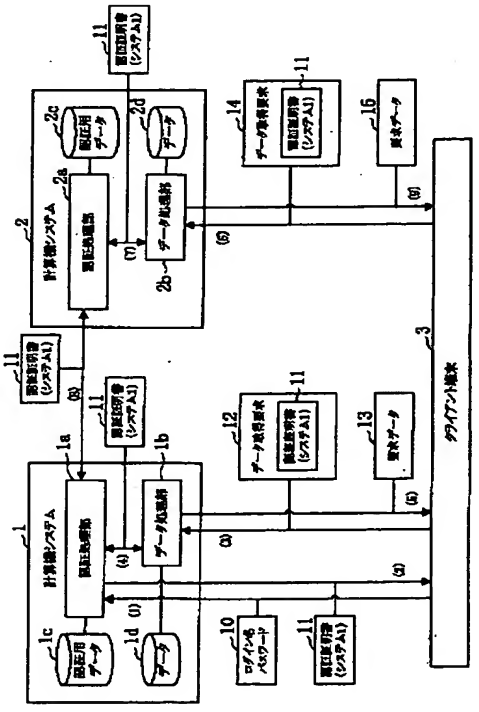
(72)発明者　花木　三良
東京都千代田区大手町二丁目3番1号　日本電信電話株式会社内

(74)代理人　100064621
弁理士　山川　政樹

最終頁に続く

(54)【発明の名称】認証システム

(57)【要約】
【課題】　クライアント端末が複数の計算機システムにアクセスする場合に２回以上の認証作業を不要とするとともに、認証専用の計算機システムを新たに設置することを不要とする。
【解決手段】　第１の記憶装置と、認証処理を行う第１の認証処理部とを備えた第１の計算機システムと、第２の記憶装置と、認証処理を行う第２の認証処理部とを備えた第２の計算機システムとを有し、第１および第２の認証処理部は、認証処理が成功した場合に所定の認証証明書をユーザに発行するとともに、ユーザが認証証明書を通知して第１または第２の計算機システムにアクセスした際に、この認証証明書の発行元の計算機システムに照会することによって認証証明書の正当性を判定し、正当である場合にアクセスを許可し、正当でない場合にアクセスを拒否する。



【特許請求の範囲】

【請求項１】　認証用データを格納した第１の記憶装置と、クライアント端末からの認証要求に応じて前記認証用データを参照して認証処理を行う第１の認証処理部とを備えた第１の計算機システムと、

認証用データを格納した第２の記憶装置と、ユーザからの認証要求に応じて前記認証用データを参照して認証処理を行う第２の認証処理部とを備えた第２の計算機システムとを有し、

前記第１および第２の認証処理部は、

前記認証処理が成功した場合に所定の認証証明書を前記ユーザに発行するとともに、前記ユーザが前記認証証明書を通知して前記第１または第２の計算機システムにアクセスした際に、この認証証明書の発行元の計算機システムに照会することによって前記認証証明書の正当性を判定し、正当である場合に前記アクセスを許可し、正当でない場合に前記アクセスを拒否することを特徴とする認証システム。

【請求項２】　請求項１に記載の認証システムにおいて、

前記第１および第２の計算機システムは、ＩＰ網を介して通信を行うことを特徴とする認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、認証システムに関し、特にクライアント端末から複数計算機システムに対してアクセスする際に用いられる認証システムに関するものである。

【０００２】

【従来の技術】従来、複数計算機システムを扱う端末は、計算機システムごとに認証の手続きを行うか、あるいはすべての計算機システムへの認証処理を一元的に管理する認証専用の計算機システムを介して、計算機システムに接続する必要があった。

【０００３】図２、図３は、従来例を示すシステム構成図である。図２は計算機システム毎に認証手続きを行うシステムであり、図３は認証を一元的に管理する認証システムを備えた従来例を示す。まず、図２に示すようにユーザのクライアント端末１０３、１０４は、計算機システム１，２にアクセスする場合、それぞれ個別に認証手続きを行わなければならない。また図３に示すようにこの従来例では、集中管理型の認証システム１０５を設けているため、認証システム１０５を介してのみ計算機システム１０１，１０２にアクセスすることができる。

【０００４】

【発明が解決しようとする課題】しかしながら、計算機システム毎に認証の手続きを行う方法では、何度もログイン処理を行わなければならず、クライアント端末を扱うユーザに負担がかかるという問題がある。

【０００５】また、認証専用の計算機システムを介して行う方法では、すべての認証要求が一旦認証専用の計算機システムに集中するため認証処理に時間がかかる。また、認証専用の計算機システム内に、アクセス先の計算機システムの全ユーザの認証用データを保持する必要があり、データ更新等の管理に手間がかかるという問題がある。

【０００６】本発明は、上述したような従来の複数計算機システムへの認証方法の有する問題点に鑑みてなされたものであり、クライアント端末が複数の計算機システムにアクセスする場合に２回以上の認証作業を不要とするとともに、認証専用の計算機システムを新たに設置する必要のない認証システムを提供することを目的とする。

【０００７】

【課題を解決するための手段】このような目的を達成するために、本発明に係る認証システムは、認証用データを格納した第１の記憶装置と、クライアント端末からの認証要求に応じて前記認証用データを参照して認証処理を行う第１の認証処理部とを備えた第１の計算機システムと、認証用データを格納した第２の記憶装置と、ユーザからの認証要求に応じて前記認証用データを参照して認証処理を行う第２の認証処理部とを備えた第２の計算機システムとを有し、前記第１および第２の認証処理部は、前記認証処理が成功した場合に所定の認証証明書を前記ユーザに発行するとともに、前記ユーザが前記認証証明書を通知して前記第１または第２の計算機システムにアクセスした際に、この認証証明書の発行元の計算機システムに照会することによって前記認証証明書の正当性を判定し、正当である場合に前記アクセスを許可し、正当でない場合に前記アクセスを拒否する。また、前記第１および第２の計算機システムは、ＩＰ網を介して通信を行ってもよい。

【０００８】このように構成することにより本発明は、ユーザの計算機システムへの認証時に認証ＯＫ（認証成功）ならばユーザに対して認証ＯＫの認証証明書を返し、認証ＮＧ（認証失敗）ならば認証証明書を発行しない。ユーザは以降の複数計算機システムへのアクセス時に、この認証証明書をアクセス要求に付加することによって自らのアクセスの正当性を示すことができる。アクセス要求を受けた計算機システムは、認証証明書が他の計算機システムで発行されたものである場合、この認証証明書を発行した計算機システムに対して正当性を照会し、照会ＯＫならばクライアントのアクセスを許可する。したがって、ユーザが行うログイン名等を用いた認証要求は１回のみであり、また各計算機システムは自システムにおける認証用データのみを保持すればよい。

【０００９】

【発明の実施の形態】次に、本発明の一つの実施の形態について図を用いて説明する。図１は、本発明の一つの実施の形態を示すシステム構成図である。同図に示すよ

うに計算機システム１は、認証処理部１ａと、データ処理部１ｂと、認証用データを格納した記憶装置１ｃと、計算機システム１が提供するデータ（文字、画像または音声情報等のコンテンツ）を格納した記憶装置１ｄとを備えている。同様に計算機システム２は、認証処理部２ａと、データ処理部２ｂと、認証用データを格納した記憶装置２ｃと、計算機システム２が提供するデータ（文字、画像または音声情報等のコンテンツ）を格納した記憶装置２ｄとを備えている。クライアント端末３は、社内ＬＡＮまたはインターネット等のＩＰ網を介して計算機システム１，２にアクセス可能であり、計算機システム１，２から提供されるデータを読み出したり、計算機システム１，２に対してデータを送信することができる。

【００１０】次に、本実施の形態の動作について説明する。まず、クライアント端末３は、ユーザのログイン名およびパスワード１０を入力することにより、計算機システム１に対して認証処理要求を行う（１）。計算機システム１の認証処理部１ａは、クライアント端末３から送られたログイン名およびパスワード１０を自らが管理する認証用データと照らし合わせ、認証ＯＫ／ＮＧの判断をする。認証ＯＫならば認証処理部１ａは、クライアント端末３に対して計算機システム１の認証証明書１１を返送する（２）。この認証証明書１１は認証が成功したことを保証するデータが記載されており、例えば認証を行ったサーバの名前や認証されたユーザの名前等が記載されている。また、認証証明書１１を暗号化することにより、不正に認証証明書１１が盗み出された際に悪用されることを防ぐことができる。なお、認証方法は上記に限られるものではなく、指紋や網膜等のユーザの身体の特徴を利用したものでもよいし、認証カードを利用した方法を用いてもよい。

【００１１】計算機システム１から認証証明書１１を受けたクライアント端末３は、この認証証明書１１を添付したデータ取得要求１２を計算機システム１へ通知する（３）。データ処理部１ｂはクライアント端末３からのデータ取得要求１２に対して、添付されている認証証明書１１が、確かなものかを発行者である認証処理部１ａに問い合わせ、認証処理部１ａが正しいと判断した場合（４）、クライアント端末３が要求するデータ（要求データ１４）をクライアント端末３に対して送信する（５）。

【００１２】クライアント端末３は、計算機システム２へのアクセス時にも上記同様に、計算機システム１が発行した認証証明書１１を添付したデータ取得要求１５を計算機システム２に通知する（６）。計算機システム２のデータ処理部２ｂは、計算機システム１が（４）で行ったのと同様に添付された認証証明書１１が確かなものかを発行者である計算機システム２の認証処理部２ａに問い合わせる（７）。

【００１３】問い合わせを受けた認証処理部２ａは、この認証証明書１１が計算機システム１が発行したものであることから、インターネット等のネットワークを介して計算機システム１の認証処理部１ａに対して認証証明書１１の正当性を問い合わせる。認証ＯＫならば（８）、計算機システム２のデータ処理部２ｂへ認証ＯＫの回答を行い（７）、認証ＯＫの結果を受けたデータ処理部２ｂはクライアント端末３が要求するデータ（要求データ１８）をクライアント端末３に送信する。

【００１４】以上により、本実施の形態では最初の１回だけログイン名およびパスワードを使って認証処理を行うが、次回からの認証処理においては認証証明書１１を使って行われるためログイン名等の再入力が不要となり、ユーザの負担を軽減させることができる。また、他の計算機システムで発行された認証証明書であっても、発行元の計算機システムに照会することによって容易にその正当性を確認することができ、複数計算機システムにおいても本実施の形態を適用することができる。

【００１５】

【発明の効果】以上、述べたように本発明によれば、複数計算機システムを一つのクライアント端末で操作するユーザはログイン名等の入力による２回以上の認証処理を不要とする。また、認証専用の計算機システムを新たに設置する必要がなく、当然のことながら、全計算機システムにおけるユーザの認証用データを１箇所（認証専用の計算機システム）で管理する必要はない。

【図面の簡単な説明】

【図１】　本発明の一つの実施の形態を示すシステム構成図である。

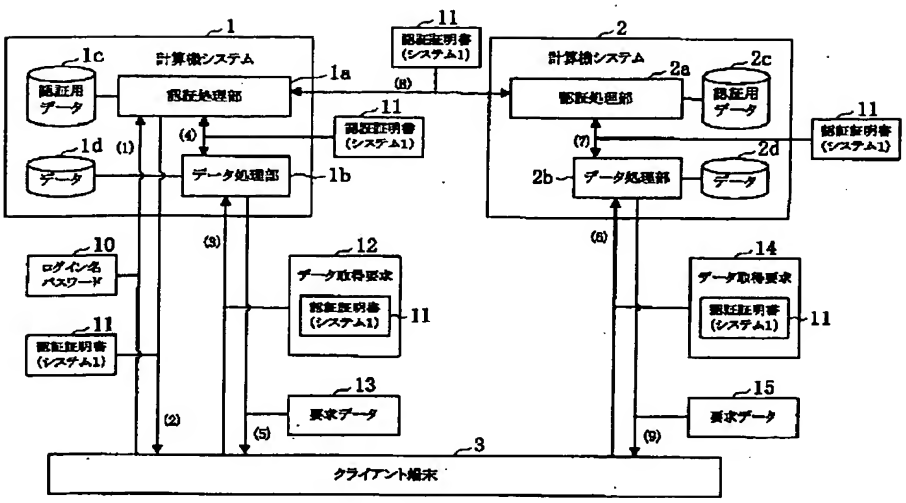
【図２】　従来例を示すシステム構成図である。

【図３】　従来例を示すシステム構成図である。

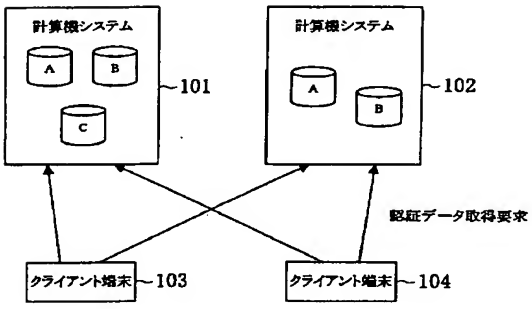
【符号の説明】

１、２…計算機システム、１ａ，２ａ…認証処理部、１ｂ，２ｂ…データ処理部、１ｃ，２ｃ…記憶装置（認証用データ）、１ｄ，２ｄ…記憶装置（データ）、３…クライアント端末、１０…ログイン名およびパスワード、１１…認証証明書、１２…データ取得要求、１３…要求データ、１４…データ取得要求、１５…要求データ。

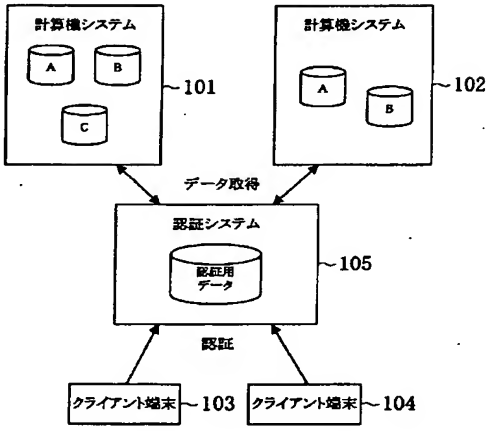
【図１】



【図２】



【図３】



フロントページの続き

(51) Int.Cl.⁷	識別記号	F I	テーマコード（参考）
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ

Ｆターム（参考）　5B045 BB12 BB19 BB28 BB47 GG09
5B085 AE03 AE23 BG07
5J104 AA07 KA01 KA17 KA19 MA03
NA01 NA05